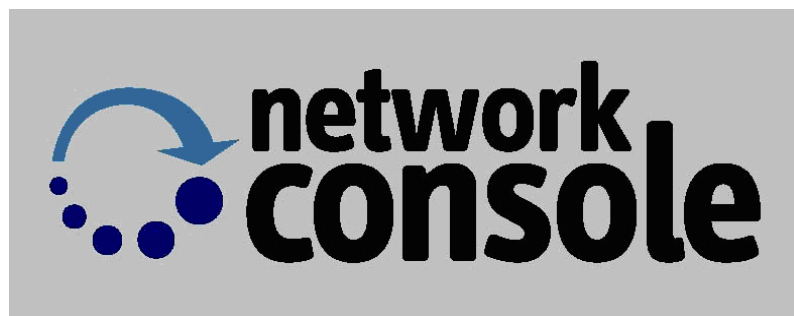




LogMeIn Network Console User Guide

April 2007

1. About the Network Console.....	2
2. Downloading and Installing the Network Console	2
3. Licensing	2
4. Network Console Features Guide	3
5. Quick Start Wizard	3
6. User Interface.....	4
7. Network & Subnet Scans	5
8. Quick Connect.....	7
9. Operations	8
10. Remote Install/Uninstall and Upgrade.....	10
11. Enterprise Configuration & Replicate Configuration	12
12. Certificate Manager	17
13. Wake On LAN	19
14. MSI File Configuration.....	20
15. Host Monitoring	21
16. Network Console Settings	22
17. Command Line Arguments	23
18. Using the Network Console with LogMeIn	25

1. About the Network Console

If you manage a significant number of RemotelyAnywhere and/or LogMeIn installations, then the Network Console presents a number of considerable advantages for you.

You probably know that one of the foremost advantages RemotelyAnywhere and LogMeIn offer the user is that special client software is not required to access a remote machine. Once RemotelyAnywhere or LogMeIn are installed you can simply open a web browser from anywhere and access your remote machine.

But what if you need access to several machines? What if you want to push installations across your network? What if you want to copy specific configuration settings to many machines at one time? This is where the Network Console comes into its own.

This guide takes you through the various features of the Network Console with the detailed information you'll need to get the most out of this advanced network management tool.

2. Downloading and Installing the Network Console

You can download the Network Console from the LogMeIn website, [here](#).

To install, download and run the installer.

Please note that the Network Console also works with LogMeIn.

3. Licensing

The Network Console is a licensed product, meaning you have to obtain your own license to use it. You can obtain a license by either purchasing one or getting a 30-day trial license.

Trial License

Fill out our registration form and install the product. When you run the product for the first time the following will occur: after the installation it will connect to our server and download a trial license. If your registration is successful, the Network Console will receive the license and install it as a background service. If you don't have a valid license it will prompt you to enter it at startup.

Purchasing a License

You can buy your license from one of our RemotelyAnywhere resellers. You can find contact information for our resellers in this documentation or on the RemotelyAnywhere website. After you receive your license, copy and paste it into the license dialog box.

Changing and Entering the License

Network Console will not start until you enter a valid license. If you already have a valid license and you want to change it (for example, you have a trial version, and you've purchased the product), you can copy and paste the new license by choosing "License" under the "Help" menu.

4. Network Console Features Guide

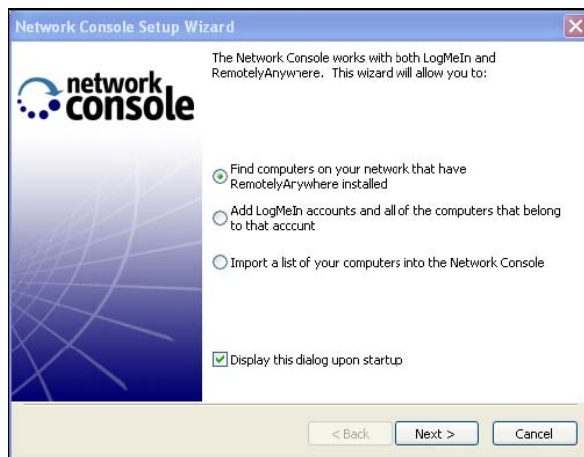
Important Note for LogMeIn IT Reach users: Not all of the Network Console's functionality is available for LogMeIn IT Reach. Please review the table below to see which features apply to RemotelyAnywhere, and which to LogMeIn IT Reach. The specific features that apply to a particular product are also indicated next to the chapter headings of this guide.

For detailed instructions on how to use the Network Console with LogMeIn IT Reach, please see the "Using the Network Console with LogMeIn™" section at the end of this guide.

<u>Network Console Feature</u>	<u>Remotely Anywhere</u>	<u>LogMeIn IT Reach</u>
Quick Start	✓	✓
Network & Subnet Scans	✓	
Quick Connect	✓	
Remote Control	✓	✓
Telnet	✓	
File Transfer	✓	✓
Open RemotelyAnywhere	✓	
Open LogMeIn		✓
Open My Computers Page		✓
Remote Install/Uninstall and Upgrade	✓	✓
Enterprise & Replicate Configuration	✓	
Certificate Manager	✓	
Wake on LAN	✓	
MSI File Configuration	✓	
Host Monitoring	✓	✓
Command Line Arguments	✓	✓

5. Quick Start Wizard

The Wizard prompts you to select one of the following three options:

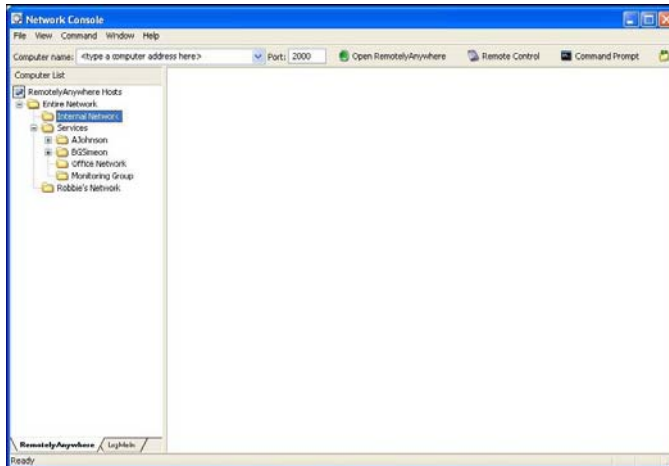


1. Find computers on your network that have RemotelyAnywhere installed.
2. Add LogMeIn accounts and all the computers that belong to that account.
3. Import a list of your computers into the Network Console.

To perform any of these functions, simply click to select the option you want and follow the Wizard instructions. After you've performed one function, you can return to the beginning of the Wizard to select another. Please also note that you can perform any of the functions listed in the Wizard from within the Network Console user interface (See sections 7 and 16 below).

6. User Interface

Once you have selected and used an option on the Wizard, the Network Console's user interface will appear:



The menu items are grouped at the top of the screen, while a list of machines on your network is displayed under **Computer List** on the left side. Please note that the available menu items correspond to the computers selected on the Computer List (if a particular menu item cannot be used for the computers selected, they will appear grayed out). The rest of the screen is taken up by the main content window, where you can access the machines listed on the left and perform other Network Console functions.

Using the options under Window in the menu items you can modify the display properties of the windows open in this main content area. Content windows can be tiled or cascaded, as well as freely resized.

The RemotelyAnywhere machines listed in the Computer List field are labeled as follows:

- Workstation without RemotelyAnywhere installed
- Workstation with RemotelyAnywhere installed
- Workstation on which it cannot be determined whether RemotelyAnywhere is installed
- Server without RemotelyAnywhere installed
- Server with RemotelyAnywhere installed

Quick Launch Toolbar

The quick launch bar allows easy access to the main features of your most recently used functions, and is displayed at the left of your browser window. The Quick Launch toolbar buttons for RemotelyAnywhere include Remote Control, File Transfer, Command Prompt, and Open RemotelyAnywhere. For LogMeIn these buttons include Remote Control, File Transfer, and Open LogMeIn. The buttons are placed right under the main menu. You can hide the toolbar under the View menu item's Quick Launch Toolbar option. The toolbar appears as follows:

Computer Name Stores the 10 most recently used computer names. You can select one of them, or type in a new one (with LogMeIn you can only enter Computer names that already exist on the Computer List). **Port Number** Contains the port number of the RemotelyAnywhere server you would like to connect to. If you select a computer name in the combobox, the port number will be pre-filled automatically with the proper value. **Open RemotelyAnywhere (or Open LogMeIn), Remote Control, Command Prompt, File Transfer** Allows you to connect to the computer name + port number you just selected.

7. Network & Subnet Scans

Network Scan

This option will search your Windows network for domains and computers on which RemotelyAnywhere is already installed. During the scan your current login credentials are used. It is recommended that you run the scan with an Administrator account.

You can also choose from the following search options:

- Search for all kinds of computers
- Search for computers with RemotelyAnywhere installed
- Search for computers without RemotelyAnywhere installed

The results of the scan will be displayed in the Computer List field on the left of the Network Console. The machine status is labeled according to the icons shown in the above User Interface section of this document, so you'll know at a glance whether it's a server or a workstation, and whether or not RemotelyAnywhere is already installed (if this can be determined during the scan.)

The check-box shown within Search Options allows you to choose whether or not to only search for domains during your scan.

Subnet Scan

With a Subnet Scan you can scan an IP address range for existing RemotelyAnywhere installations.

You are given the choice of scanning all addresses within a given subnet address, or within a given address range (specified in the **From To** and fields). You can further refine your search to resolve host names, and only show machines on which RemotelyAnywhere is already installed.

The additional search options are the same as for the Network Scan, detailed above, with the additional option to resolve host names. This box is checked by default.

Again, the results of the scan will be displayed in the Computer List field on the left.

Export Computer List

Here you have the option to export your Computer List section to a “.reg” file. The stored computers and folders will be written to a file containing all the settings saved into the predefined section including your computer’s passwords. The format of the file satisfies the Windows “.reg” file requirements.

Import Computer List

Here you have the option to import previously exported hosts to the Computer List section. There are two ways to do this:

Option 1 Shut down the Network Console and double click on the .reg file in Windows Explorer to import the file into the registry. Note: In this case all your other saved information will be lost because it will be overwritten by the imported hosts.

Option 2 Run the Network Console and use the Import Computer List... option under the “File” menu. In this case the program will ask whether you want to overwrite your existing.

After you’ve made your selections for either a Subnet or Network scan, click Next to choose your authentication preferences. The Network Console will query each remote host for useful data, including the following:

- **RemotelyAnywhere listening port**
- **RemotelyAnywhere version**
- **The RemotelyAnywhere installed path**
- **Operating system version**
- **Computer description**
- **The MAC address of the computer’s network adapter**

These data are queried by the RPC (Remote Procedure Call), which can only function when the Network Console has been authenticated on the remote host. You can select your authentication preferences for RPC calls in the dialog box:

- **Use the current logon credentials**
 - Select this option and the Network Console will the scan the remote computer with credentials of the user that is currently logged on. The query will fail if the specified user does not have logon rights on the remote machine.

- **Use the following username\password for all target computers**
 - The Network Console will scan the remote computers using the specified username and password (including the domain) combination.
- **Save this login information...**
 - Check this box and the specified authentication method will be saved for each target computer in the Computer List section, enabling faster access to the computer for future remote control, file transfer, etc. sessions.

Note: All passwords are encrypted and stored in the computer's registry and memory. If you export your predefined section it will also automatically export all your stored passwords (encrypted, of course). Only the person who exports the passwords can import them, and only on the specified computer. You have to use the same account to perform this function, otherwise your passwords again. This only applies to your stored passwords, as the other settings can be imported again.

8. Quick Connect

To quickly connect to a machine running RemotelyAnywhere, select Quick Connect from the Quick Start dialog box or from the File menu. The following dialog box will appear (see next page):

To directly connect to a machine, enter the name of the computer to which you wish to connect, select an operation and click OK. The available operations are:

- **Remote Control**
- **Telnet**
- **File Transfer**
- **Open RemotelyAnywhere**

The selected option for session type will determine the contents of the main area..

Quick connect

Computer name: Port:

Login

Use SSL to connect ☒

Use NTLM for authentication ☒

Password authentication

Username:

Password:

Domain:

Save password ☐

Session type

Remote Control ☐

Command Prompt ☐

File Transfer ☐

Open RemotelyAnywhere ☒

OK Cancel

9. Operations

Whether you use the Command option in the Menu, the Quick Connect dialog box, or the context menu in the Computer List field, many operations can be performed via the Network Console. 

Remote Control	Uninstall RemotelyAnywhere
Command Prompt	MSI File Configuration
File Transfer	Refresh
Enterprise Configuration	Remove
Replicate Configuration	Ping
Certificate Manager	Properties
Wake on LAN	Open RemotelyAnywhere
Install RemotelyAnywhere	

Remote Control

One of the central features of RemotelyAnywhere and LogMeIn IT Reach is its advanced ability to remotely control the computer on which it is installed, thus enabling you to authentically replicate the experience of sitting in front of the host computer — regardless of where you actually are in the world. When you select Remote Control, the host machine's display is shown and you can then manipulate the keyboard and mouse.

When RemotelyAnywhere or LogMeIn IT Reach is being accessed by a web browser, by default it attempts an ActiveX-based version of the remote control (for use with Internet Explorer), and, if that fails, a Java-based version. When RemotelyAnywhere is being accessed by the Network Console, a native remote control interface, based largely on the ActiveX version, is used.

Please consult the relevant section of the RemotelyAnywhere or LogMeIn IT Reach User Guide for more information on remote controlling the desktop.

Command Prompt

Using this feature you can open the command prompt on the host computer. In addition to all the Telnet functionality available when accessing a machine remotely via a web browser, the Network Console offers extra functionality through the toolbar at the top of the open window. With this toolbar you can, from left to right: mark a rectangle for selection, copy data, paste data, and view the remote clipboard (as in Remote Control above).

File Transfer

The File Transfer feature allows you to securely transfer files between the local host and the remote computer, synchronize folders, and delete and rename files. The File Transfer component looks and behaves similarly to the File Transfer component found in RemotelyAnywhere and LogMeIn IT Reach. Please consult that portion of the RemotelyAnywhere or LogMeIn IT Reach User's Guide for further information on its operation.

Remote Install, Enterprise Configuration and Replicate Configuration

These features will be dealt with separately in the next section of this document.

Refresh

If you need to make sure the most up-to-date machine properties are displayed in the Computer List field, click Refresh.

Remove

With this option you can remove a machine from the list in the Computer List field. It is also possible to select multiple machines with the Shift or Ctrl keys in order to perform operations such as Remove on several machines at once.

Ping

With this option you can ping a selected computer. If it can be pinged, then a small green icon will be displayed to the left of the computer. If it cannot, then a small red icon will be displayed.

Properties

The information under **properties** for each computer is arranged under four tabs, namely, **Connection**, **RemotelyAnywhere**, **Advanced**, and **Wake On LAN**.

Connection

Under the connection tab you can find and modify a computer's name, port number, any comments, and login information. Inside login group you can specify whether the Network Console user should use SSL to connect and whether NTLM is used for authentication. If this default setting is deselected the required password authentication fields become available for editing.

RemotelyAnywhere

Here you can see its path on the host machine, and which version of RemotelyAnywhere is installed. Saved settings such as screen resolution and network speed are also displayed on the following page.

Advanced

Under the advanced tab you can find whether it is a workstation or a server. The OS version and a description can also be found as well as a record of any errors.

Wake On LAN

Here you can specify the MAC address, Network Address, and Subnet Mask of the computer to use at Wake ON LAN feature. The MAC address of the computer can be automatically detected with the determine button.

Open RemotelyAnywhere

Finally, you can simply open up RemotelyAnywhere's normal web interface and gain access to all the remote tools that would normally be available to you when accessing RemotelyAnywhere through a web browser. This is also the default action if you double click on a machine name in the Computer List field.

You can simultaneously open as many computers' RemotelyAnywhere interfaces as you like when using the Network Console, as they will each occupy a window in the main content frame.

10. Remote Install/Uninstall and Upgrade

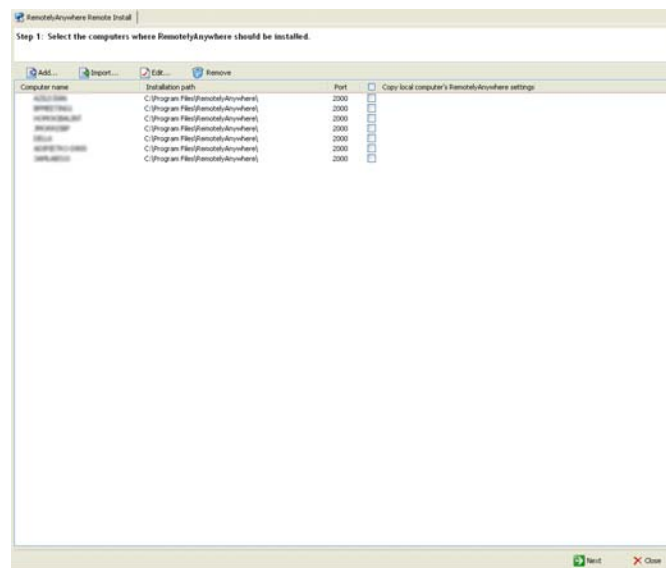
One of the most useful functions of the Network Console, besides keeping track of and accessing the RemotelyAnywhere or LogMeIn installations on your network, is the additional functionality for installing RemotelyAnywhere or LogMeIn on remote machines.

Installing RemotelyAnywhere

To install RemotelyAnywhere remotely, right-click on a computer or group of computers in the Computer List field on the left and select Install RemotelyAnywhere, or use the option in the Command menu. This is a four-step procedure:

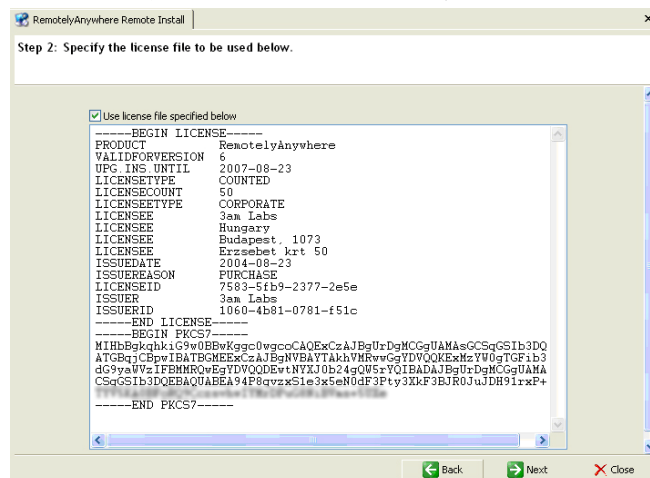
Step 1

The target computer is shown in the field at the top, with name, installation path and port. You can add, edit or remove machines with the buttons directly above the listed computers.



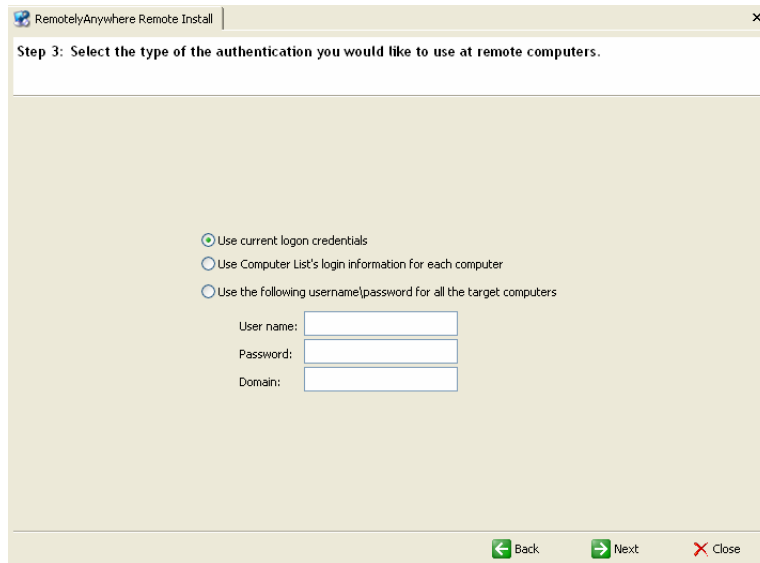
Step 2

The license displayed in the bottom-most field will be used if you check the box for it to do so. (Please ensure you copy and paste the entire license text as you received it in the text file!)



Step 3

Click **Next** and a dialog box appears that prompts you to enter authentication details for the remote installation:


Step 4

When you click the **Next** button, the Network Console will install or upgrade RemotelyAnywhere on the selected machines.

Requirements for Remote Installations and Upgrades

These conditions must be met in order to remotely install RemotelyAnywhere using the Network Console:

1. RemotelyAnywhere needs to be installed on the machine on which you're running the Network Console.
2. The local user on the client must be an Administrator on the remote host or must have a valid Administrator account on the remote host.

Uninstalling RemotelyAnywhere

To uninstall RemotelyAnywhere remotely, right-click on a computer or group of computers in the Computer List field on the left and select Uninstall RemotelyAnywhere, or use the option in the Command menu. This is a four-step procedure:

Step 1: The name of the target computer(s) is shown in the field at the top, along with the option to delete RemotelyAnywhere files after the uninstallation.

Step 2: Click **Next** and a dialog box appears that prompts you to enter authentication details for the remote uninstallation.

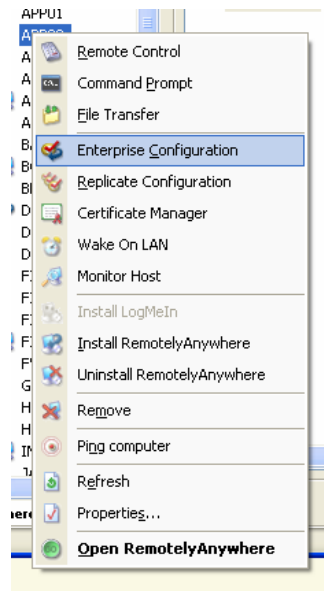
Step 3: When you click the **Next** button, the Network Console will uninstall RemotelyAnywhere from the selected machine(s).

11. Enterprise Configuration & Replicate Configuration

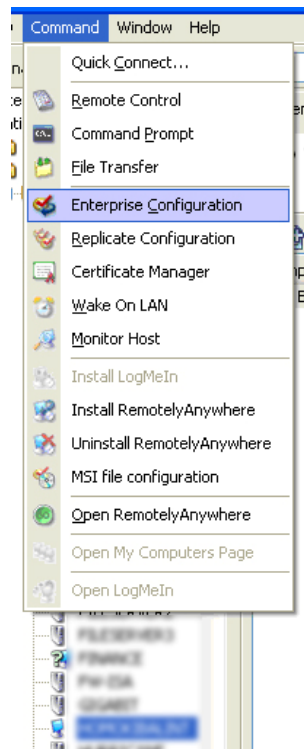
Enterprise Configuration

Using the Enterprise Configuration option in the Network Console you can push your desired configuration settings to multiple machines across your network quickly and easily.

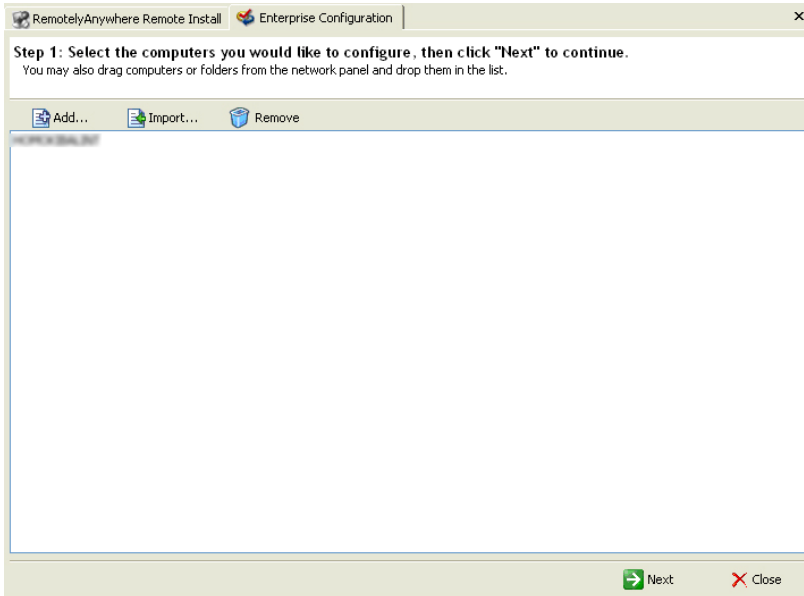
Select the computers for configuration from the Computer List field on the left hand side of the screen. Then right-click and select Enterprise Configuration...



...or select this option under Command in the main menu:



The Enterprise Configuration tab page will appear in the main content window, as shown here:



This tab page allows you to do the following things:

Add new computers to the list

There are three different ways you can do this. You can press Add button and enter the computer name manually, you can drag and drop computers from the Computer List field or you can import a list of computers from a file by clicking on the Import host list... button. Please note that such a list should be a text file containing one computer name or IP address per line.

Remove computers from the list

This is done by selecting them and clicking **Remove**.

Cancel the process

This is done by clicking **Close**.

Click **Next** and a dialog box appears, prompting you to enter authentication details for the remote enterprise configuration:

RemotelyAnywhere Remote Install Enterprise Configuration

Step 2: Select the type of the authentication you would like to use at remote computers.

☒ Use current logon credentials
☐ Use Computer List's login information for each computer
☐ Use the following username/password for all the target computers

User name:
 Password:
 Domain:

Click **Next**, and on the following screen you will be able to configure the various settings according to your needs. You will notice that some fields have default values already entered. These represent the merged configuration settings that already existed on the selected machines.

Enterprise Configuration

Step 2: Set the configuration values then click "Next" to continue.

Computer list

- Appearance
- Network
 - Advanced
- Access control
- Colors
- Log settings
 - Advanced Log settings
- ODBC messages
- License
- Remote Control
 - Advanced
- Telnet Server
 - Client
- SSH Server
 - Advanced SSH Settings
- IP Address Lockout
- IP Address Filter
- Advanced Options

Computer list

You are configuring the following computers:

DEMO4-W2KS
DEMO5-XPPRO

The default values are calculated as follows: When you clicked **Next** on the previous screen the Network Console queried the configuration settings from the selected machines. A single value was merged as follows: The Network Console checked if the setting were the same on all machines. If YES this is the value shown. If NO then the checkboxes will be grayed out, strings will display empty fields, and combination boxes will be shown in an undefined state.

Types of Values

Three state checkboxes representing Boolean values: **Checked**: the values will be written to all computers with the value TRUE (1). **Unchecked**: the values will be written to all computers with the value FALSE (2). **Grayed**: this value will be skipped, and will remain the same on all computers.

Input fields for representing string values. The values in fields left blank will not be written to the target machines.

Combo box If you select <diverse> the value will be skipped.

List view Gray items will be skipped and black items will be written to all computers.

Tree view Gray items and all their descendants will be skipped. Black items and all their descendants will be written to all computers.

Configuration Categories

For a detailed reference of what the various configuration categories mean we advise you to refer to the appropriate parts of the RemotelyAnywhere User's Guide (in the chapters on Security and Preferences). They are listed here for your reference with added notes where there is additional functionality (or different usage) from that detailed in the RemotelyAnywhere User's Guide.

Computer list: Here you can see a list of the computers you are currently configuring. It is not possible to add or remove machines from this list. Doing so would necessitate restarting the Enterprise Configuration process from the beginning.

Appearance: You can set the custom HTTP directory and the custom HTTP index file here.

Network: (General) and Network advanced (SMTP and Dynamic IP support)

Access Control

Colors

Systray Settings

Log Settings

OBDC Settings License

Remote Control and Remote Control Advanced

Telnet Server and Telnet Server Advanced

SSH Server

IP Address Lockout

IP Address Filter: The IP address filters are displayed in a tree view. There are two types of item. The IP profile item encapsulates a certain amount of IP filters. You can define several IP profiles, but only one of them can be active. The active IP profile can be switched on the Network configuration page. A new one can be added by typing its name into the Profile names field, and clicking on the Add button. An IP filter item can be added by clicking on the Add... button.

Deploying the configured values: Finally, you can deploy the values you have configured by clicking the Deploy configuration... >> button in the bottom right corner.

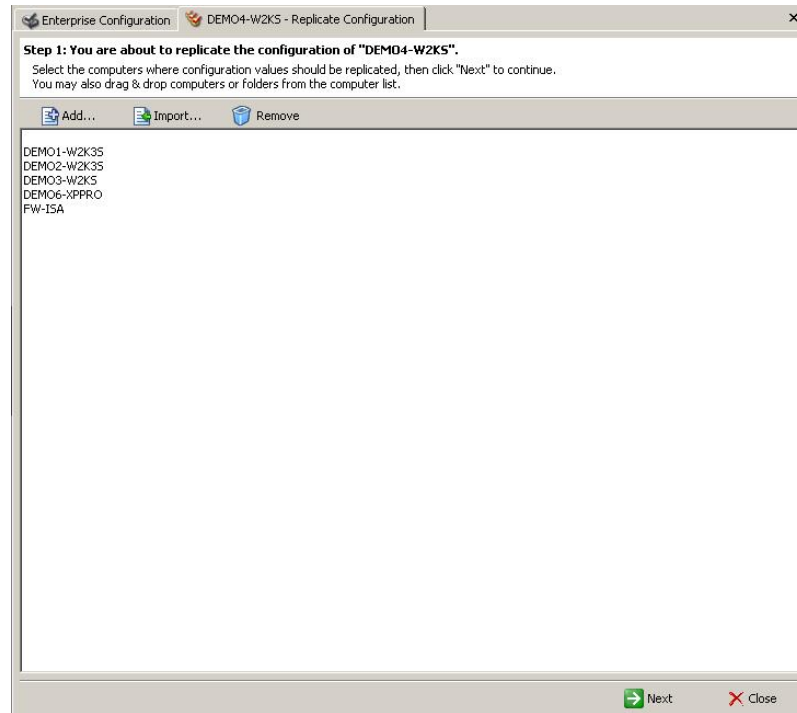
Replicate Configuration

The Replicate Configuration option is a one-to-many configuration distribution tool. It is typically used to distribute a fine-tuned RemotelyAnywhere configuration to a selected group of computers.

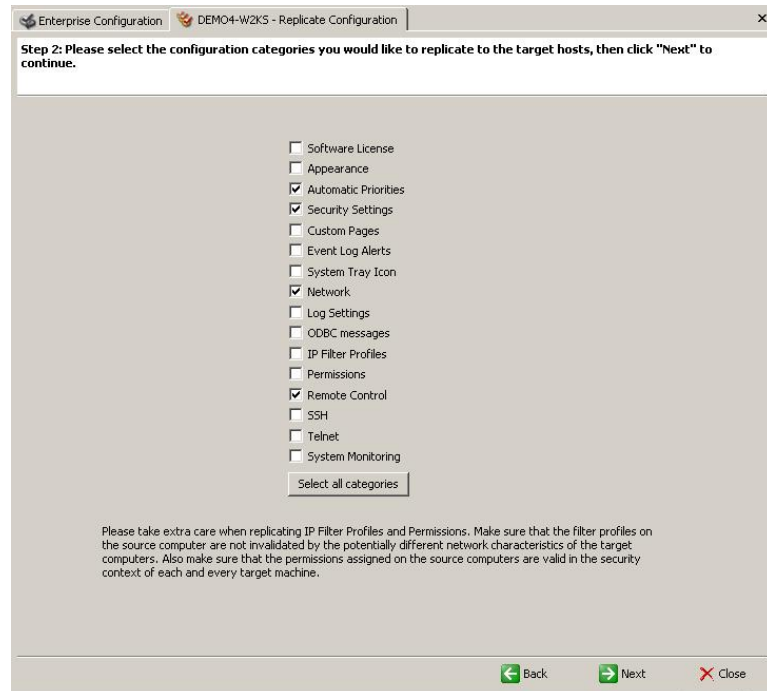
First select the source computer from the Computer List field and select Replicate Configuration, either by right clicking or from the Command option in the main menu. Having done this, the Replicate Configuration page will be displayed in the main content window.

Step 1: The source computer's name will be displayed in the title bar of the main content window. You can add destination computers for the replicated configuration settings in 3 ways.

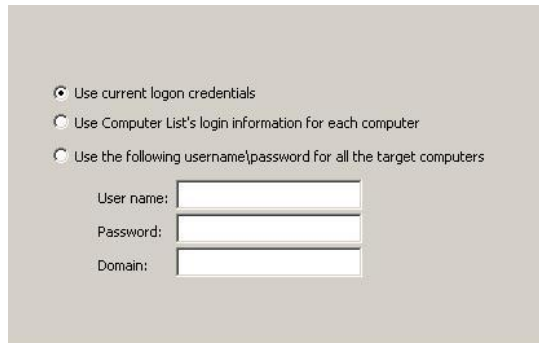
You can enter the computer name by clicking on the Add button and enter the name manually into the upcoming dialog box, you can drag and drop computers from the Computer List field or you can import a list of computers from a file by clicking on the **Import host list** button. Again, please note that such a list should be a text file containing one computer name or IP address per line.



Step 2: Before starting replication, you should select at least one configuration category from the checkbox menu that appears in the next dialog box. These categories are the same as those detailed above under Enterprise Configuration.



Step 3: Click **Next** and a dialog box will appear prompting you to enter authentication details for the remote replicated configuration:



A dialog box with a light gray background. It contains three radio buttons for authentication options:

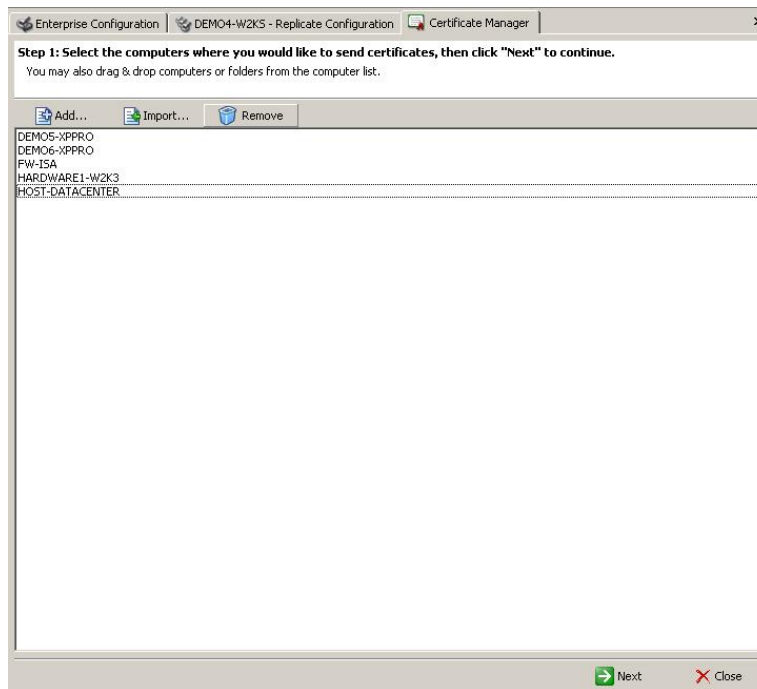
- ☒ Use current logon credentials
- ☐ Use Computer List's login information for each computer
- ☐ Use the following username/password for all the target computers

 Below the radio buttons are three text input fields labeled "User name:", "Password:", and "Domain:".

Finally, by clicking the Next button the status page will be displayed and you will be able to trace the replication process.

12. Certificate Manager

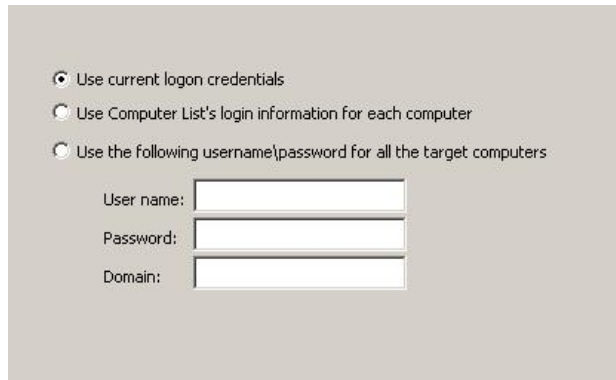
This option allows you to retrieve security certificates from a Certificate Server on your network and copy them to the certificate store on one or multiple RemotelyAnywhere-installed computers on the same network.



By using this option, the browser on your client computer will not prompt you about an unknown Certificate Authority (CA) every time you make a secure connection to RemotelyAnywhere. Your client browser will instead recognize the CA certificate and automatically identify the computer you are connecting to. If you install the certificate and establish a secure connection, no warning messages will mean that the connection is verified and you are in fact entering your login credential into a computer you have chosen to trust.

To use this feature, simply do the following:

Step 1: Click **Next** and a dialog box will appear prompting you to enter authentication details for the remote replicated configuration:

A screenshot of a dialog box with a light gray background. It contains three radio button options for authentication. The first option, 'Use current logon credentials', is selected. Below the options are three text input fields labeled 'User name:', 'Password:', and 'Domain:'.

☒ Use current logon credentials
☐ Use Computer List's login information for each computer
☐ Use the following username\password for all the target computers

User name:
Password:
Domain:

Step 2: Select the type of authentication you would like to use, then click **Next**. (Note: the authentication must be valid for all the computers you select.)

Step 3: The Console will display the Certificate Servers it has detected on the network on a drop-down list. Select the Certificate Server from which you want to retrieve certificates for copying, then click **Next**.

The Console will deploy the certificates from the Certificate Server to the certificate stores of the selected computers. If there are no certificate servers running on the network, you will receive the message: *There are no certificate servers on your network.*

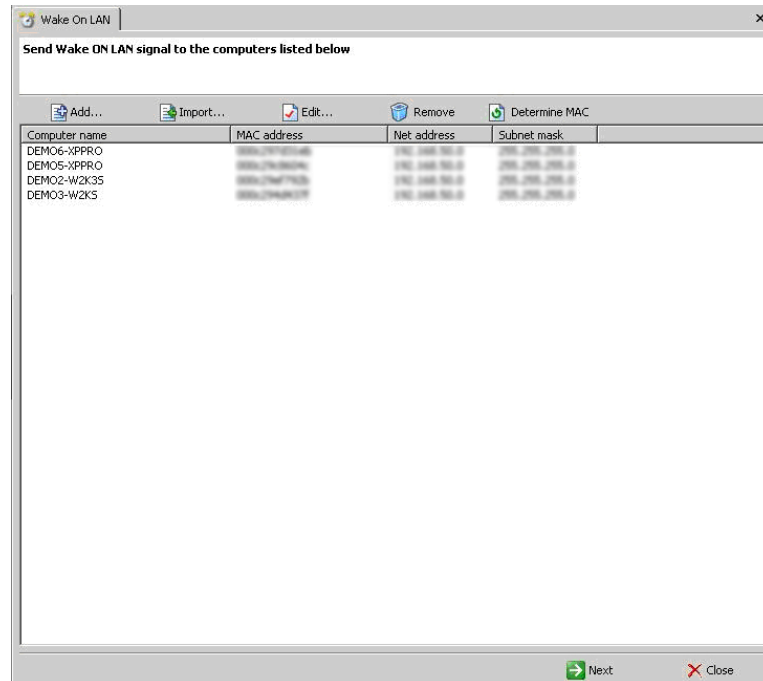
Note: the certificate service is included in Windows 2003 Server, and can be added in **Windows > Add/ Remove programs**.

13. Wake On LAN

By using the Wake On LAN feature you can send “magic packets” to your computers that are switched off to get them back online.

To use this feature, first select the computers you would like to wake up:

Add new computers to the list: There are three different ways you can do this. You can 1) press the **Add** button and enter the computer name manually; 2) drag and drop computers from the **Computer List** field; or 3) import a list of computers from a file by clicking on the **Import host list...** button. Please note that the list should be a text file containing one computer name or IP address per line.



You also must determine the **MAC** address of all the computers in the list. To do this, click the **Determine MAC** button. If the **MAC** address cannot be resolved automatically, highlight the computer, click **Edit**, and enter the address manually, or remove the computer from the list before proceeding. The Net Address and Subnet Mask fields indicate the network the remote computer resides on.

If each computer has its MAC address, NetAddress and Subnet mask triple specified, the Console sends out the “magic packets” to prompt the computers to come online.

Note: The Wake On LAN functionality only works with computers that have a Network card/mainboard that supports Wake On LAN. This feature is enabled under the network card settings.

Enabling Wake on LAN in Windows XP

1. Select **My Network Places** on Windows Start menu and then right-click to select **Properties**.
2. On the Network Connections page select your network adapter and right-click **Properties**.
3. Click **Configure** on the Local Area Connection Properties dialog box.
4. Your network card's configuration dialog box will appear. Select the **Power Management** tab and check **Allow this device to bring the computer out of standby**.

14. MSI File Configuration

This feature allows you to pre-define RemotelyAnywhere settings in the installation binary itself. When RemotelyAnywhere is deployed using the modified MSI, it will use the settings specified in the binary file, saving you from having to re-configure every installation after the fact.

This feature is useful because it allows you to deploy multiple RemotelyAnywhere installations with identical configurations in accordance with the rules of your network environment.

Note: Changing the MSI file this way will invalidate the LogMeIn digital signature on the installation binary. The executables contained within will remain individually signed.

To use this feature, simply do the following:

Step 1: Select **MSI File Configuration** from the **Command** drop-down menu. Alternatively, you can right-click on a computer or group of computers in the left-side navigation pane and select **MSI File Configuration**.

In the main display area, you will be prompted by the Browse button to select the RemotelyAnywhere installation file (ra*.msi) file to configure. Click **Next**.

Step 2: You will be prompted to select and configure the .msi's values in a navigation tree that appears in the main display area. The listed values include:

- **Appearance:** Here you can tailor to your liking the look of RemotelyAnywhere installations that are deployed from the configured .msi file.
- **Network > Advanced** Here you can configure TCP/IP port settings, in addition to settings for IP filtering, limits for File Transfer downloads, and HTTP Tunneling.
- **Access Control** Here you can set user permissions for RemotelyAnywhere on installations that are deployed from the configured .msi file.
- **Colors** Here you set the color scheme for the RemotelyAnywhere interface on installations that are deployed from the configured .msi file.
- **Log settings > Advanced Log settings** Here you can modify the general settings for RemotelyAnywhere and the Syslog settings.
- **ODBC messages** Allows you to configure how messages from RemotelyAnywhere's System Monitoring and Scripting features are written to a database. The configurable values include **Data Source**, **User name & Password** for access to the data source, and the **Table Name** for the table in which the messages are to be stored.
- **License** Here you can view the license on the selected .msi file, or paste an alternative RemotelyAnywhere license for the eventual installation(s).
- **Remote Control > Advanced** Here you can set preferences for how the host computer behaves while it is being controlled remotely. Options include whether to disable the host keyboard and mouse, blank the host's monitor, and automatic clipboard size, among others.
- **Telnet Server > Client** Here you can specify which port / address you want RemotelyAnywhere to listen on for telnet connections. This defaults to the standard telnet port of 23, and all available interfaces. Changes take effect when the service is restarted.
- **SSH Server > Advanced SSH Settings** As with the Preference options for the Telnet Server, this dialog box allows you to view and modify SSH-related options. The IP and address options are the same as above, but with the default port of 22, which is standard for SSH connections. Changes will take effect when the service is restarted.
- **IP Address Lockout** Use this setting to detect and temporarily lock out potential intruders on the host computer(s) on which you eventually install RemotelyAnywhere. This security precaution allows you to configure two specific types of filter. These are called the Denial of Service Filter and the Authentication Attack Filter.

- **IP Address Filter** Allows you to specify exactly which computers are allowed to access RemotelyAnywhere on your system.
- **Advanced Options** Here you can set advanced preferences such as whether to disable HTML-based remote control, enabling debug-level logging and HTTP content compression, and customized login messages.

Click any of the listed values to configure them. At the bottom of the main display area, you can also select to load the default values for the .msi file or import the configuration settings from another RemotelyAnywhere-installed computer on your network.

Click Next to set the configuration of the .msi file.

Step 3 The location of the configured .msi file will be displayed in the main display area. To deploy the .msi, simply copy it to one of multiple computers and initiate its installation.

15. Host Monitoring

Host Monitoring (also available for LogMeIn machines with the Network Console version 6.20.130) allows you to interactively monitor your CPU and memory usage, screen content, interactive users, number of connections, etc. To use this feature, select the computers you would like to monitor and right-click **Monitor Host**.

You can choose to monitor your computers under a Thumbnail or List View.

The following data are displayed automatically under Host Monitoring:

- Screen content
- CPU usage
- Memory usage
- Interactive user
- Remote time
- Number of RemotelyAnywhere connections.

Host Monitoring Features

- **View:** Click this button on left on the toolbar to select the List of Thumbnails View.
- **Sort:** Click this button to sort the computers listed under Host Monitoring (by CPU Usage, Memory Usage, Interactive User, Remote Time, Number of RemotelyAnywhere Connections, User Defined). You can sort by clicking on the column header in List View mode, or by selecting **sort base** in the drop-down menu (second toolbar button from left).
- **Add new computers to the list:** There are two different ways to add computers. You can 1) click the **Add** button and enter the computer name in the dialog box, or 2) drag and drop computers from the **Computer List** field.
- **Remove computers:** Select the computer your wish to remove and click **Remove**.
- **Switch on/off detailed view:** Under Detailed View you can see detailed information about the computer, including a larger screenshot, CPU history and memory usage. Click the Detailed View button to switch this view on or off.
- **Reconnect to a computer:** If a connection has ended due to an error, you can reconnect to the remote computer by double clicking the computer's thumbnail, or by selecting **Reconnect** in the pop-up menu.
- **Open RemotelyAnywhere:** Opens up the computer's RemotelyAnywhere window.
- **Remote Control:** Starts a remote control session with the selected computer.
- **File Transfer:** Starts a file transfer session with the selected computer.
- **Command Prompt:** Starts a command prompt session with the selected computer.

- **Refresh screenshot:** Allows manual refresh of the screenshot. You can also set a screenshot refresh time interval in the settings dialog box.
- **Host Monitoring settings:** To set the Host Monitoring settings, click the Settings button on the toolbar. You can also find these features on the main menu under Host Monitoring.

Host Monitoring Settings

Load host monitoring page at startup: Check this box to automatically display the computers you monitored during your previous Hosting Monitoring session.

Automatically download screenshot: Check this box to have the screenshots taken from the computers in the time interval of your choosing. **Note:** this interval must be between 5 and 7200 seconds.

16. Network Console Settings

Under **View > Settings** in the menu you can modify the default settings for the Network Console itself. The dialog box that is displayed organizes the information under four tabs.

Workspace: Under the Workspace tab you can select to have the Console perform the following actions on startup under the On startup section:

- **Display Quickstart wizard:** Check this box to have the Quickstart wizard display itself automatically upon startup of the Network Console.
- **Automatically expand last used LogMeIn account:** Check this box to have the Console automatically expand the list of computers linked to the LogMeIn account that was last used on the Console.

To set the Network Console's security settings, look under the Security section:

- **Display SSL warning dialog box at "Add new host" command:** Check this box to have the Console display an SSL warning dialog box when the **Add new host** command is used.
- **Display warning dialog box when a non-secure connection is not supported by the target host:** Check this box to have the Console display a warning message when the target host detects and does not support a non-secure connection.
- **Warn about invalid site certificates:** Check this box to have the Console display a message warning of invalid security certificates.
- **Warn about certificate revocation:** Check this box to have the Console display when a target host's security certificates have been revoked.

Host Monitor: See Host Monitoring section above (Section 12)

LogMeIn: Two options are displayed under the LogMeIn tab, under **Account Maintenance**:

- **Automatically refresh expanded LogMeIn accounts:** Check this box to have the Console automatically refresh **LogMeIn** accounts at a time interval of your choosing.
- **Remove unknown computers from the list:** Check this box to have the Console to remove unknown computers from the list.

Proxy: Under the **Proxy** tab you can specify the proxy server to use when the Network Console needs to access the Internet. If the proxy server requires authentication, you need to fill the username and password fields as well. You can also manually set up proxy settings by filling in the **Proxy username** and **Proxy password** fields. In addition, you can click the **Get proxy settings** and **Test proxy settings** tabs, respectively, to retrieve and test the current proxy settings.

17. Command Line Arguments

Usage: RAConsole [command <parameter1> <parameter2> .. <parameterN>]

Valid commands are:

remotecontrol [-computer COMPUTER] [-port PORTNR]
 [-login USERNAME] [-pass PASSWORD] [-domain DOMAIN] [-ntlm] [-ssl]
 Opens a RemoteControl session on computername:port.

- You must specify a computername (-computer).
- If you do not specify a port number (-port), 2000 is assumed.

telnet [-computer COMPUTER] [-port PORTNR]
 [-login USERNAME] [-pass PASSWORD] [-domain DOMAIN] [-ntlm] [-ssl]
 Opens a Telnet session on computername:port.

- You must specify a computername (-computer).
- If you do not specify a port number (-port), 2000 is assumed.

filetransfer [-computer COMPUTER] [-port PORTNR]
 [-login USERNAME] [-pass PASSWORD] [-domain DOMAIN] [-ntlm] [-ssl]
 Opens a FileTransfer session on computername:port.

- You must specify a computername (-computer).
- If you do not specify a port number (-port), 2000 is assumed.

openra [-computer COMPUTER] [-port PORTNR]
 [-login USERNAME] [-pass PASSWORD] [-domain DOMAIN] [-ntlm] [-ssl]
 Opens a RemotelyAnywhere session on computername:port.

- You must specify a computername (-computer).
- If you do not specify a port number (-port), 2000 is assumed.

installra [-computers COMPUTER1, COMPUTER2, .. , COMPUTERN]
 Installs RemotelyAnywhere onto remote computers

- You do not have to specify a computer

enterpriseconfig [-computers COMPUTER1, COMPUTER2, .. , COMPUTERN]
 Opens an Enterprise Configuration session with the specified computers

- You do not have to specify a computer

wakeonlan [-computers COMPUTER1, COMPUTER2, .. , COMPUTERN]
 Opens a Wake On LAN session with the specified computers

- You do not have to specify a computer

replicateconfig [-computerfrom COMPUTERFROM] [-computersto COMPUTERTO1, COMPUTERTO2, .. ,
 COMPUTERTON]
 Opens a ReplicateConfig session

- You must specify a source computer (-computerfrom)
- you do not have to specify the target computer(s) (-computersto)

openlmi [-computer COMPUTERTNAME] [-description DESCRIPTION] [-hostid HOSTID]
 Opens a LogMeIn session to the specified computer.

- The computer must have been previously added to your computer list.

lmiremoterontrol [-computer COMPUTERTNAME] [-description DESCRIPTION] [-hostid HOSTID]
 Opens a remote control session to the specified computer.

- The computer must have been previously added to your computer list.

lmifiletransfer [-computer COMPUTERTNAME] [-description DESCRIPTION] [-hostid HOSTID]
 Opens a file transfer session to the specified computer.

- The computer must have been previously added to your computer list.

openmycomputers [-email EMAIL]
 Opens the My Computers page of the specified account.

Valid parameters are:

computer COMPUTER

The machine to perform an operation on.

port PORTNR

Specify the HTTP listener port for RemotelyAnywhere.

login USERNAME

Specify the name of the user to connect.

pass PASSWORD

User's (-login USERNAME) password.

domain DOMAIN

Specify the domain to which the user (-login USERNAME) belongs.

ntlm

Use NTLM authentication for connection

ssl

Use SSL encryption for the specified connection

computers COMPUTER₁, COMPUTER₂, .. , COMPUTER_N

Computer list to perform an operation on.

computerfrom COMPUTERFROM

Machine to perform an operation on.

computersto COMPUTERTO₁, COMPUTERTO₂, .. , COMPUTERTON

Computer list to perform an operation on.

description DESCRIPTION

Description that uniquely identifies a LogMeIn -**computers** COMPUTER₁, COMPUTER₂, .. ,

COMPUTER_N

computerfrom COMPUTERFROM

computersto COMPUTERTO₁, COMPUTERTO₂, .. , COMPUTERTON

description DESCRIPTION

Description that uniquely identifies a LogMeIn host from your Computer List section

hostid HOSTID

The unique identifier of the LogMeIn host that have been generated by the LogMeIn Gateway.

email EMAIL

The email address that is associated with an account.

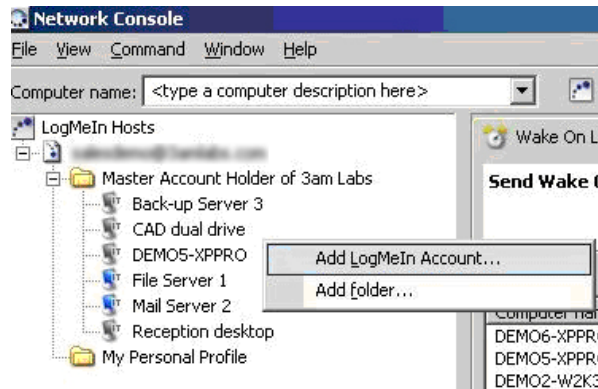
18. Using the Network Console with LogMeIn

The Network Console integrates seamlessly with **LogMeIn**, LogMeIn's gateway-based remote access solution for computers outside the LAN. This integration allows you to quickly access host computers on your network that have LogMeIn installed, much in the same way that you would access those installed with RemotelyAnywhere.

Individual LogMeIn accounts are listed by their email addresses on the Network Console's **Computer List** navigation bar, where they appear under the **LogMeIn Hosts** menu tree item. All host computers linked to a specific LogMeIn account appear as sub-items below the specified account's e-mail address.

Adding a LogMeIn Account to the Navigation Bar

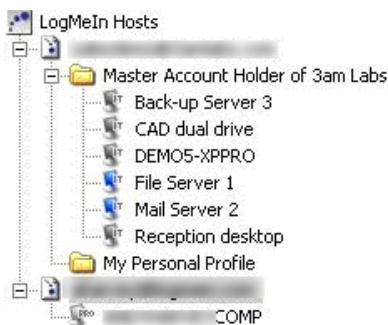
Step 1: Right-click on LogMeIn Hosts on the navigation bar and select **Add LogMeIn Account**.



Step 2 : Enter the LogMeIn account login information (the e-mail address and password used to remotely access the specified hosts). You can also check Save Password to allow quicker remote access to the computer in the future.

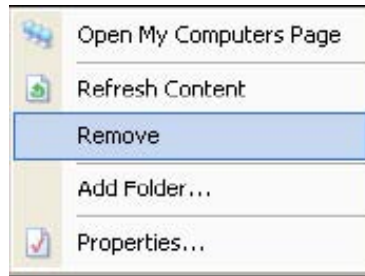
Step 3: The Network Console will query the computers added to the specified LogMeIn account. A small status bar will appear at the bottom of the Computer List navigation bar. To cancel this operation, click Cancel.

Once the operation is completed the added computers will appear as sub-items below the email address of the specified LogMeIn account:



Removing a LogMeIn Account from the Computer List

Right-click on the email address of the LogMeIn account and select **Remove**.



Refreshing the Status of a LogMeIn Account

Right-click on the email address and select the Refresh Content option.

The status of the computers added to a specified LogMeIn account is automatically maintained by the Network Console. The status includes the version of LogMeIn installed on the host computer:

-  **LogMeIn IT**
-  **LogMeIn Pro**
-  **Unknown LogMeIn version**
-  **LogMeIn Free** (Note: Host computers that have the free version of LogMeIn installed are not accessible via the Network Console.)



An “X” superimposed over the host computer’s icon is displayed if the host is not remotely accessible (for example, because the machine is switched off.)

Note: The Network Console automatically lists all host computers attached to a LogMeIn account once you add that account to the Computer List. Any changes you make to the list of host computers (as displayed on the specified account’s My Computers page in LogMeIn) are mirrored automatically on the corresponding list displayed by the Network Console.

Properties

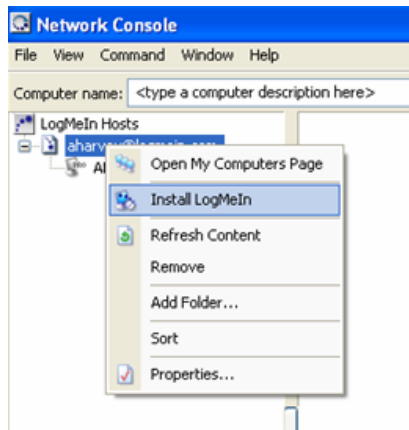
To view the properties of a host computer installed with LogMeIn, right-click on the computer and select the Properties option. The following dialog box is displayed:

Step 2: Next, right-click on a computer or group of computers in the Computer List field on the left and select Install LogMeIn, or use the option in the Command menu.

Step 3: The target computer is shown in the field at the top, with name, installation path and port. You can add, edit or remove machines with the buttons on the bottom. You can also select to use the LogMeIn settings of the machine you are sitting at for the remote installation.

Step 4: Enter your LogMeIn credentials in the next window, then click to select which version of LogMeIn you would like to install: LogMeIn Pro, LogMeIn Pro Trial, LogMeIn IT Reach or LogMeIn IT Reach Trial. Click Next.

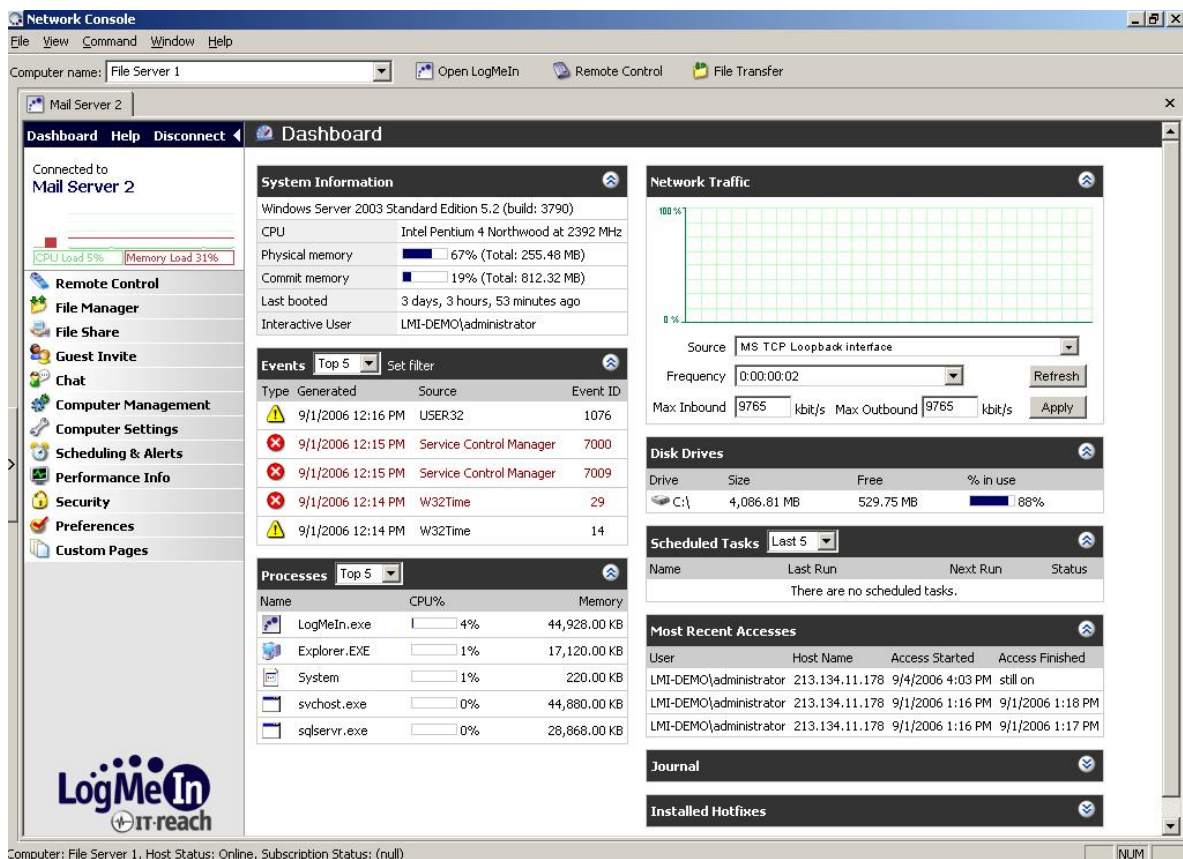
Step 5: Select to use the current logon credentials for the remote installation, the Computer List’s login information for each computer, or enter a username and password for all the target computers.



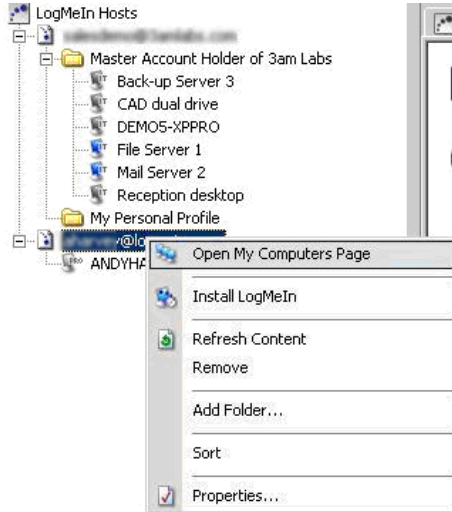
Step 6: When you click the Next button, the Network Console will install LogMeIn on the selected machines.

Other LogMeIn Options

Connect to a computer directly: To directly connect to a host computer installed with LogMeIn (without having to enter its login credentials), double-click on the computer. Its desktop will be displayed on the Network Console. (Note: you cannot use this functionality to access host computers installed with the free version of LogMeIn.)



Open My Computers page: Right-click on the selected account and select the Open My Computers Page option:



If no login information for the selected computer has been saved, or if this is the first time you've connected to the computer remotely, you will be prompted to enter the information in the following dialog box:

Check the **Save login information** box to save the login information under the Computer List.

 A screenshot of the 'Login' dialog box. The dialog has a title bar with 'Login' and a close button. It contains two radio buttons: 'Use Windows Authentication' (selected) and 'Use LogMeIn Password Authentication'. Under 'Use Windows Authentication', there are three text fields: 'User name:', 'Password:', and 'Domain:'. Under 'Use LogMeIn Password Authentication', there is one text field: 'Password:'. There is a checked checkbox labeled 'Save login information'. Below the checkbox is a note: 'Note: If you are accessing this computer with a Windows account, check in the "Windows Authentication" radio button and fill in the user name, domain (optional) and password fields above. If you use a LogMeIn computer password to access this computer, check in the "Use LogMeIn Password Authentication" radio button and fill in the password field.' At the bottom are 'OK' and 'Cancel' buttons.